State of Utah
Technical Architecture
Wireless LAN/WAN Standard 2000.05.15
Revised 3.8.2002

Title: Wireless LAN/WAN Standard

Introduction: Wireless LANs are used within the state to provide network services in areas that are not readily served by traditional wiring methods. Wireless LANs are an enhancement to existing wired network services and *are not intended as a replacement for standard wired LANs.* This standard applies to intra-building LAN communications and extra building LAN/WAN's. Any agency desiring to implement an inter-building solution needs to coordinate with Information Technology Services (ITS) to acquire the necessary equipment under existing contracts, and implement that equipment in a secure fashion. Extra-building LAN/WAN's require coordination with the ITS WAN Planning and Security groups; Building and Facilities Maintenance groups; qualified radio planning personnel; and agency LAN administrators.

Rationale and Justification: Wireless LAN/WANs are an important part of the overall networking strategy of the State of Utah and all products used in wireless LANs across the state must be interoperable and secure.

Application: This standard is applicable to all executive government agencies in the State of Utah.

Current Architecture: The State of Utah of Utah has experimented with products from a number of different wireless LAN/WAN vendors. Because of the dynamic nature of the wireless industry, the physical environment, the applicable industry standards, and equipment must be chosen carefully.

Future Architecture: Wireless LAN/WAN devices are available from multiple vendors and are acceptable, providing that they meet the State of Utah requirements for interoperability and security as reflected in IEEE 802.11x standards. Future network connection devices will include PDA's, cellular phones and other IEEE compliant wireless network devices. High speed wireless communication as proposed by IEEE 802.11a is not expected to have widespread acceptance until dual mode access points for both 802.11b and 802.11a are available.

Definitions:
Access Point: A device that transports data between a wireless network and a wired network (infrastructure).

Authentication: Verifying the identity of a user that is logging onto a computer system or verifying the integrity of a transmitted message.

Encryption: Converting data into a secret code for transmission over a public network. The original text, is converted into a coded equivalent called "ciphertext" via an encryption algorithm. The ciphertext is decoded (decrypted) at the receiving end. The greater the number of bits in the key (cipher strength), the more possible key combinations and the longer it would take to break the code. The data is encrypted, or "locked," by combining the bits in the key mathematically with the data bits. At the receiving end, the key is used to "unlock" the code and restore the original data.

Firewall: A method for keeping a network secure from intruders. It can be a single router that filters out unwanted packets or may comprise a combination of routers and servers each performing some type of firewall processing. Firewalls are widely used to give users secure

access to the Internet as well as to separate a company's public Web server from its internal network.

LDAP: (**L**ightweight **D**irectory **A**ccess **P**rotocol) A protocol used to access a directory listing. LDAP support is being implemented in Web browsers and e-mail programs, which can query an LDAP-compliant directory. It is expected that LDAP will provide a common method for searching e-mail addresses on the Internet, eventually leading to a global white pages. LDAP is a sibling protocol to HTTP and FTP and uses the ldap:// prefix in its URL.

Multi Point: A wireless device that extends one or more wired, or partially wired networks to a separate wireless device in a separate facility (i.e. Building to building type devices).

NDS: (**N**ovell **D**irectory **S**ervices) Novell's directory service. NDS is based on the X.500 directory standard and is LDAP compliant. NDS maintains a hierarchical database of information about the network resources within a global enterprise, including networks, users, subgroups, servers, volumes and printers. NDS users log into the network as a whole, not a specific server, and NDS determines their access rights.

Non-routable Network: An IP (Internet Protocol) network addressing system that, by definition and Internet standard, the addresses are not forwarded by Internet gateways, and are therefore, private.

Proxy: A "proxy" or "application level gateway," it is an application that breaks the connection between sender and receiver. All input is forwarded out a different port, closing a straight path between two networks and preventing a cracker from obtaining internal addresses and details of a private network.

Radio Frequency (RF) Terms (GHz, MHz, Hz): The international unit for measuring frequency is Hertz (Hz), which is equivalent to the older unit of cycles per second. One Mega-Hertz (MHz) is one million Hertz. One Giga-Hertz (GHz) is one billion Hertz.

RADIUS: (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) is an access control protocol that uses a challenge/response method for authentication.

Roaming: Movement of a wireless node between two microcells. Roaming usually occurs in infrastructure networks built around multiple access points.

VPN: (Virtual Private Network): A private network that is configured within a public network. VPNs enjoy the security of a private network via access control and encryption, while taking advantage of the economies of scale and built-in management facilities of large public networks.

WEP: The 802.11 standard describes the communication that occurs in wireless local area networks (LANs). The Wired Equivalent Privacy (WEP) algorithm is used to protect wireless communication from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network; while not an explicit goal in the 802.11 standard, it is frequently considered to be a feature of WEP. WEP relies on a secret key shared between a station and an access point (ie. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit. The 802.11x standard does not discuss how the shared key is established.

Wireless Local Area Network (WLAN): A LAN technology relying on transmission over the air typically in an unlicensed frequency such as the 2.4GHz band. Wireless access points (base stations) are connected to an Ethernet hub or server and transmit a radio frequency over an area of several hundred to a thousand feet which can penetrate walls and other non-metal barriers. Roaming users can be handed off from one access point to another like a cellular phone system.

Wireless Node: A user-computing device with a wireless network interface card (adapter).

Authority: *Utah Code Section 63D Information Technology Act*.

National and International Standards References: The IEEE 802.11x standard defines the protocol for Ad-hoc and client/server networks. An Ad-hoc network is a simple network where communications are established between multiple stations in a given coverage area without the use of an access point or server. The standard specifies the etiquette that each station must observe so that they all have fair access to the wireless media. It provides methods for arbitrating requests to use the media to ensure that throughput is maximized for all of the users in the base service set. The client/server network uses an access point that controls the allocation of transmit time for all stations and allows mobile stations to roam from cell to cell as The access point is used to handle traffic from the mobile radio to the wired or wireless backbone of the client/server network. This arrangement allows for point coordination of all of the stations in the basic service area and ensures proper handling of the data traffic. The access point routes data between the stations and other wireless stations or to and from the network server. Typically WLANs controlled by a central access point will provide better throughput performance.

Additional Wireless LAN Standards information, including the full text of IEEE 802.11b, and working documents related to emerging IEEE 802.11x standards is available from the Wireless LAN Association (WLANA) at http://www.wlana.com/intro/standard/index.html.

Technical Requirement(s): All products that conform to the IEEE 802.11x standard must have a software upgrade path to conform to the changes and additions to the standard as they become available.

Security Requirement(s): All implementation of WLAN's will conform to the following security practices and to the requirements established by the developing 802.11i wireless security standard when it is released:

- By definition in the State Network Access Policy, WLANs are untrusted and are subject to the same connection restrictions as any other untrusted network, accordingly its network access point will be controlled by ITS, IP packet flow into the state WAN will be restricted. Connect the WLAN as an outside network—a firewall, or system running firewall software will be required to restrict IP access between WLAN and the inside network (the rest of the LAN, and the State WAN). Pursuant to the State Network Access policy, the installation of the WLAN will "restrict the physical and logical connections to centralized entry points to facilitate the monitoring for known intrusions, controlling the flow of network packets, authentication of users and authorization to resources will be managed by the Division".

- The IP addressing scheme for the WLAN shall be non-routable IP addresses as follows:
  1. Class A: **10.x.x.x**
  2. Class B range: **172.16.0.0-172.31.0.0**
  3. Class C range: **192.168.0.x-192.168.254.x**

- For added security and due to the non-routable nature of the IP addressing of the WLAN, Web access for the WLAN will be available only using a proxy server.

- Encryption between the nodes and access points will be set to the maximum level the technology will permit. Users of 40-bit encryption will upgrade to a minimum of 128-bit encryption as soon as practicable.

- User Authentication must validate and be unique to the user. Example, the user should authenticate to a secure directory (such as NDS or LDAP) using a secure protocol (such as RADIUS)

- Access to the internal network must be specific and controlled. Permission to internal resources, such as the mapping of drives, will require validation of the user and access through VPN client software.

- No default configuration settings can be allowed on the WLAN hardware

- The WLAN hardware should be configured to use dynamic WEP (Wired Equivalent Privacy) keys, renegotiating at an interval frequent enough to prevent their derivation by an intruder.

- All WLAN hardware will be configured by appropriately trained and designated personnel prior to connecting to the State WAN, with permission granted by ITS, including, but not limited to, telecommuting connections in private residences.

- Wireless clients will not operate in "peer-to-peer", or ad hoc mode.

- WLAN's will be independently audited on a random basis. ITS reserves the right to disable non-complying networks upon discovery and until they comply with this standard.

Exceptions: Any wireless LAN/WAN that is in place as of April 1, 2002, and approved by ITS may continue to be used. If at any time the existing LAN/WAN is upgraded, moved, or changed it shall then meet in full this Wireless LAN/WAN Standard. ITS may conduct independent audits on a random basis and if the LAN/WAN is found to be a safety or security risk, ITS will then require that the LAN/WAN be upgraded to meet this Standard.

Gap Analysis: Existing intra-building wireless LAN/WAN's in the State of Utah in testing or under current development are already in compliance with this standard.

Migration and Implementation Plan: All new purchase of Wireless LAN/WAN products will be expected to be in full compliance with this standard from any of the vendors offering compliant products.

Review Cycle: This standard will be reviewed and updated on an annual basis, based upon the CIO approval date.

State Purchasing Contracts: Wireless LAN/WAN products are available from multiple vendors under the following State contracts:

Contract Number	Description	Vendor
AR-1191	LAN/WAN Switching Equipment	Consonus
AR-887	Cisco Aironet Wireless Equipment	Consonus
AR-Pending	WSCA Wireless LAN Products	Western States Contracting Alliance Vendors

All wireless contracts will require ITS authorization before WLAN products can be procured by agencies. Effective 1/1/02 PC Stores contractors may no longer provide WLAN or LAN/WAN switching equipment.

References:

Interim Date: May 15, 2000
Organization Sponsoring the Standard: ITS Network Planning Group
State Technical Architect Approval Date: May 18, 2000
CIO Approval Date: May 18, 2000
ITPSC Presentation Date: May 18, 2000
Author(s): Robert Woolley, Joe Leary, Floyd Ritter (ITS)

Revised Interim Date: December 10, 2001
Revision Team: Robert Woolley, Rick Gee, Floyd Ritter, David Lee (ITS), SISC
Revision Sponsoring Organization(s): ITS Network Planning Group, SISC, CIO
State Technical Architect Revision Approval Date: Pending
CIO Revision Approval Date: Pending
ITPSC Revision Final Presentation Date: March 28, 2002
Related Documents: Security Executive Order, State Information Security Policy; State Network Access Policy; IEEE 802.11x standards, and RFC 1918.
Review Cycle: Annual